FortiNAC

Set Admin Privileges Based On Directory Groups

Version: 8.x

Date: 8/28/2018

Rev: C

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET KNOWLEDGE BASE

http://kb.fortinet.com

FORTINET BLOG

http://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

http://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTINET COOKBOOK

http://cookbook.fortinet.com

FORTINETTRAINING AND CERTIFICATION PROGRAM

http://www.fortinet.com/support-and-trainingt/training.html

NSE INSTITUTE

http://training.fortinet.com

FORTIGUARD CENTER

http://fortiguard.com

FORTICAST

http://forticast.fortinet.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

Tuesday, August 28, 2018

Set Admin Privileges Based On Directory Groups

To provide access to the FortiNAC user interface you can place Administrative Users in special groups that set the appropriate privileges. Typically this is done for users in your Directory, by placing them in special groups within the directory that correspond to matching groups in FortiNAC. When the Directory is synchronized with FortiNAC, users in the appropriate groups will be given Administrator or Administrative privileges based on their group settings and the Admin Profile Mapping that matches the user's group.

Note: The Domain Users Group cannot be used to set Admin privileges because user details for users in that group are not populated in FortiNAC when directory synchronization is done.

Implementation

Directory

1. Integrate your Directory with FortiNAC. See online topic Authentication Directories for configuration and integration information.
2. Temporarily disable the Directory Synchronization task in the FortiNAC Scheduler to prevent the synchronization from pulling directory information before the setup is complete. See online topic Scheduler View.
3. If you want to send e-mail to Admin users, make sure to map the e-mail field in your directory to the e-mail field in Network Sentry. To set up this mapping go to **System > Settings > Authentication > LDAP**. Select the directory and click Modify. Select the Attribute Mappings tab and make sure that the e-mail field is configured. This setting allows users to receive e-mails based on Device Profiling settings, Guest Manager settings, and event to alarm mappings based on group membership. See online topic Add/Modify Directory - User Attributes Tab.
4. Create groups in the directory for each set of administrator privileges you wish to grant. For example, if you want to have Administrative Users with full rights to FortiNAC and Administrative Users who are just Sponsors for guest access, create two groups in the directory, one for each type of Administrative Users. Add the appropriate Administrative Users to the new groups.
5. Make sure the new groups are selected to be included when the directory and FortiNAC are synchronized. To select the groups go to **System > Settings > Authentication > LDAP**. Select the directory and click Modify. Click the Select groups tab and review the selected groups. See online topic Add/Modify Directory - Select Groups Tab.

FortiNAC

1. Navigate to **Users > Admin Profiles** and create the appropriate Admin User Profiles. All Administrative Users require an Admin Profile that provides permissions. See online topic Admin Profiles And Permissions.
2. Navigate to **System > Groups** and create Administrator groups to contain the users who will be given access to FortiNAC. The group name must be absolutely identical to the name of the group in the directory. See Online Help topic Add Groups.

   Note: Since groups automatically brought over from the directory are typically Host groups, you must create the Administrator groups manually. If a group already exists with the name of one of the Administrator groups, you must delete that group and add it again as an Administrator group.
3. Navigate to **Users > Admin Profiles** and Map Administrator Groups to Admin Profiles. These mappings allow FortiNAC to determine the Admin Profile that should be associated with an Administrative User based on the group that contains that user. Mappings are ranked and Administrative Users are associated with the first mapping they match. See Online Help topic Admin Profile Mappings.

   Example:

   - Administrative User John is in **Group A** and **Group B**.
   - **Group A** is mapped to a Guest Sponsor Profile and Ranked **#5**.
   - **Group B** is mapped to a Device Manager Profile and Ranked **#2**.
   - FortiNAC associates John with the Device Manager Profile because that mapping has a higher Rank and is the first match for John.
4. Navigate to **System > Scheduler** and enable the Directory Synchronization task. Run the task to update the groups.
   - Users that have already registered in FortiNAC are updated immediately.
   - New users that are not in the FortiNAC database but do exist in the Directory are added to FortiNAC groups when they log into the Admin User Interface the first time.
5. Navigate to **System > Groups** and verify that the correct users have been placed in each group. See Online Help topic Groups View.
6. Navigate to **Users > Admin Users** and verify that the Admin User Profile is correct for each user. See Online Help topic Admin Users.

Important: If the root account for FortiNAC is placed in a group with an Admin User Profile other than the Administrator Profile, the Admin Profile of this account will change. This could potentially leave you without a root or admin login that provides access to the entire FortiNAC product.

Important: Aging for new Administrative Users created by being added to a directory group is determined by Global Aging settings. See Aging and Aging Out Host Or User Records.